UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/458,921	12/10/1999	MOHAMMAD PEYRAVIAN	P-4541.001	9480

24112 7590 03/11/2004

COATS & BENNETT, PLLC
P O BOX 5
RALEIGH, NC 27602

EXAMINER	
VAUGHAN, MICHAEL R	

ART UNIT	PAPER NUMBER
2131	9

DATE MAILED: 03/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/458,921	PEYRAVIAN ET AL.	
	Examiner	Art Unit	
	Michael R Vaughan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 December 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Detailed Action

Claims 1-50 have been examined and are pending.

Response to Arguments

Applicant's arguments, see pages 12-14, filed 1-26-04, with respect to the rejection(s)of claim(s) 1-49 under USC 102(b) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of newfound prior art.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1-14, 29-36, and 41-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al (USP Re. 34,954) in view of Schneier (Applied Cryptography).

As per claim 1, Haber et al teach:

Receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document (column 2, line 55—column 3, line 10);

Creating at said outside agency a time stamp receipt based on said identifying data and a time indication (column 2, line 55—column 3, line 10);

Transmitting said time stamp receipt and said message authentication code to a designated party (FIG. 1, block 19);

Haber et al fails to explicitly teach generating a message authentication code (herein MAC) based on said time stamp receipt and a secret key. Schneier teaches that the use of MAC's as a way to prove that a document has not been forged or altered (pages 455-459). MAC's are well known in the art and have many uses. Only hashing the same exact document with the same secret key will generate a new MAC that matches the saved MAC. Using a MAC has some advantages in security. Only the entity that creates a MAC can validate the MAC if the secret key used to create the MAC belongs to the entity. It would be advantageous to generate a MAC based upon the time stamp receipt and a secret key because it would allow the person wanting to validate the time stamp (presumably not the owner) to interact with a trusted outside agency first hand. This would remove any doubt about the origin of a receipt the person might have if he/she is receiving a time stamp that is already certified. The person would also have a second source of validation that none of the contents of the time stamp receipt have been altered since it was stamped. By using a MAC it would force an interaction with the outside agency at a later time in order to validate the MAC. Also the outside agency would then use a cryptographic signature scheme to generate a new MAC on the received time stamp receipt based on the same secret key and compare the new MAC with the received time stamp receipt.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the system of Haber et al because generating a MAC based upon the time stamp receipt and a secret key would provide another means to authenticate a time stamp with a trusted outside agency to further insure that the time stamp receipt had not in any way been forged or altered since the time of the signing.

As per claims 2-6, Haber et al teach a method of identifying data that comprises a hash value generated from a one-way hash function and including the hash value and the time indication to the time stamp receipt (column 3, lines 10-65).

As per claim 7, Haber et al teach said time stamp request further includes an identification number associated with the requestor (column 3, lines 10-65 column 4, lines 8-39).

As per claim 8, Haber et al teach said message authentication code comprise a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenate together (column 3, lines 10-65).

As per claim 9, Haber et al teach the step of validating said message authentication code includes recomputing said message authentication code at said

outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code (see abstract).

As per claim 10, Haber et al teach wherein the certifying step includes signing said message authentication code using a private signature key controlled by said outside agency (see abstract).

As per claim 11, Haber et al teach wherein the certifying step includes signing said time stamp receipt using a private signature key controlled by said outside agency (see abstract).

As per claim 12, Haber et al teach storing said secret key in a database at said outside agency (column 3, line 40-45). Having to remember the original number or secret key is necessary to validate one-way hash functions or MACs, which are one-way hash functions, which use a secret key. It is therefore inherent that the secret key is stored in a database where it can later be retrieved to certify a timestamp.

As per claim 13, Haber et al teach wherein each time stamp receipt includes a sequential record number that is used at said outside agency to look up said secret key in said database (column 4, lines 8-20).

As per claim 14, Haber et al teach the step of transmitting said certified time stamp receipt to said requestor (column 4, line 8-26).

As per claim 29, Haber et al teach:

Receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document (column 2, line 55—column 3, line 10);

Creating at said outside agency a time stamp receipt based on said identifying data and a time indication (column 2, line 55—column 3, line 10);

Haber et al fails to explicitly teach generating a message authentication code (herein MAC) based on said time stamp receipt and a secret key. Schneier teaches that the use of MAC's as a way to prove that a document has not been forged or altered (pages 455-459). MAC's are well known in the art and have many uses. Only hashing the same exact document with the same secret key will generate a new MAC that matches the saved MAC. Using a MAC has some advantages in security. Only the entity that creates a MAC can validate the MAC if the secret key used to create the MAC belongs to the entity. It would be advantageous to generate a MAC based upon the time stamp receipt and a secret key because it would allow the person wanting to validate the time stamp (presumably not the owner) to interact with a trusted outside agency first hand. This would remove any doubt about the origin of a receipt the person might have if he/she is receiving a time stamp that is already certified. The person

would also have a second source of validation that none of the contents of the time stamp receipt have been altered since it was stamped. By using a MAC it would force an interaction with the outside agency at a later time in order to validate the MAC. Also the outside agency would then use a cryptographic signature scheme to generate a new MAC on the received time stamp receipt based on the same secret key and compare the new MAC with the received time stamp receipt.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the system of Haber et al because generating a MAC based upon the time stamp receipt and a secret key would provide another means to authenticate a time stamp with a trusted outside agency to further insure that the time stamp receipt had not in any way been forged or altered since the time of the signing.

Transmitting said time stamp receipt and said message authentication code to a designated party (FIG. 1, block 19).

As per claims 30-34, Haber et al teach a method of identifying data that comprises a hash value generated from a one-way hash function and including the hash value and the time indication to the time stamp receipt (column 3, lines 10-65).

As per claim 35, Haber et al teach said time stamp request further includes an identification number associated with the requestor (column 3, lines 10-65 column 4, lines 8-39).

As per claim 36, Haber et al teach said message authentication code comprise a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenate together (column 3, lines 10-65).

As per claim 41, Haber et al teach:

Haber et al fails to explicitly teach generating a message authentication code (herein MAC) based on said time stamp receipt and a secret key. Schneier teaches that the use of MAC's as a way to prove that a document has not been forged or altered (pages 455-459). MAC's are well known in the art and have many uses. Only hashing the same exact document with the same secret key will generate a new MAC that matches the saved MAC. Using a MAC has some advantages in security. Only the entity that creates a MAC can validate the MAC if the secret key used to create the MAC belongs to the entity. It would be advantageous to generate a MAC based upon the time stamp receipt and a secret key because it would allow the person wanting to validate the time stamp (presumably not the owner) to interact with a trusted outside agency first hand. This would remove any doubt about the origin of a receipt the person might have if he/she is receiving a time stamp that is already certified. The person would also have a second source of validation that none of the contents of the time stamp receipt have been altered since it was stamped. By using a MAC it would force an interaction with the outside agency at a later time in order to validate the MAC. Also the outside agency would then use a cryptographic signature scheme to generate a new

MAC on the received time stamp receipt based on the same secret key and compare the new MAC with the received time stamp receipt.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the system of Haber et al because generating a MAC based upon the time stamp receipt and a secret key would provide another means to authenticate a time stamp with a trusted outside agency to further insure that the time stamp receipt had not in any way been forged or altered since the time of the signing.

As per claim 42, Haber et al teach wherein the certifying step includes signing said message authentication code using a private signature key controlled by said outside agency (see abstract).

As per claim 43, Haber et al teach wherein the certifying step includes signing said time stamp receipt using a private signature key controlled by said outside agency (see abstract).

As per claim 44, Haber et al teach the step of transmitting said certified time stamp receipt to said requestor (column 4, line 8-26).

As per claims 45 and 47, Haber et al teach certifying said time stamp receipt at outside agency comprises signing said time stamp receipt with a private signature key (column 7, line 10).

As per claims 46 and 48, the examiner supplies the same rationale for the motivation as recited in the rejection of claim 41 to incorporate the teachings of Schneier within the system of Haber et al. Haber teaches that the key is a secret key and private signature keys are often referred to as secret keys in the art of cryptography.

Claims 15-28, 37-40, 49, and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al in view of Schneier in view of Doyle (WO 99/16209).

As per claims 15, and 37-40 Haber et al teach:
Receiving a time stamp request at an outside agency at a first time, said time stamp request including identifying data associated with said document (column 2, line 55—column 3, line 10);

Creating at said outside agency a time stamp receipt based on said identifying data and a time indication (column 2, line 55—column 3, line 10);

Haber et al fails to explicitly teach generating a message authentication code (herein MAC) based on said time stamp receipt and a secret key. Schneier teaches that the use of MAC's as a way to prove that a document has not been forged or altered (pages 455-459). MAC's are well known in the art and have many uses. Only hashing the same exact document with the same secret key will generate a new MAC that matches the saved MAC. Using a MAC has some advantages in security. Only the entity that creates a MAC can validate the MAC if the secret key used to create the MAC belongs to the entity. It would be advantageous to generate a MAC based upon the time stamp receipt and a secret key because it would allow the person wanting to validate the time stamp (presumably not the owner) to interact with a trusted outside agency first hand. This would remove any doubt about the origin of a receipt the person might have if he/she is receiving a time stamp that is already certified. The person would also have a second source of validation that none of the contents of the time stamp receipt have been altered since it was stamped. By using a MAC it would force an interaction with the outside agency at a later time in order to validate the MAC. Also the outside agency would then use a cryptographic signature scheme to generate a new MAC on the received time stamp receipt based on the same secret key and compare the new MAC with the received time stamp receipt.

In view of this it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Schneier within the system of Haber et

al because generating a MAC based upon the time stamp receipt and a secret key would provide another means to authenticate a time stamp with a trusted outside agency to further insure that the time stamp receipt had not in any way been forged or altered since the time of the signing.

Haber et al are silent in disclosing encrypting the secret key with a second secret key to generate a key message. Doyle teaches encrypting a public key with a secret private key [claim 8]. Encrypting a key with a private key creates a key message, which can be validated by a public key to prove authenticity. Also this procedure removes the agency from having to remember the first private key.

In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Doyle within the system of Haber et al because it would allow the first encryption key to be encrypted with the private key of the trusted agency prevent the agency from having to remember many private keys.

Haber et al are silent in disclosing generating a second message authentication code based on the first message authentication code. Doyle teaches encrypting data associated with the certification request using the second private key [pg. 12, lines 25-26 and claim 10]. Using the private key to encrypt data, attributes the encryption to a particular author whereby the data can be validated using the public key of the owner of the private key. It would have been obvious to one of ordinary skill that the first message authentication code can be validated by using the second secret key from the teaching of Doyle (pg. 11, line 30—pg. 12, line 1).

In view of this, it would have been obvious to one of ordinary skill in the art at the time of the invention to employ the teachings of Doyle within the system of Haber et al because it would allow a second message authentication code to be created based on the first message authentication code which corresponds to a particular entity without having to remember both the first private key used and who it belongs to. Simply knowing the master private key is enough information to decrypt the message authentication code to reveal who the owner of the data is and when it was signed without revealing the plaintext. Using the private key to encrypt data, attributes the encryption to a particular author whereby the data can be validated using the public key of the owner of the private key.

From the employing of the teachings of Doyle within the system of Haber et al, it follows that:

Haber et al are silent in expressly disclosing transmitting a second message authentication code and the encrypted key message. The examiner supplies to same rationale for the motivation to incorporate the teachings of Doyle within the system of Haber et al. Therefore it would have been obvious to include the second message authentication code and the encrypted key message along with the time stamp receipt and first message authentication code to the requestor as Haber et al teach (column 2, line 55—column 3, line 10 and column 4, lines 8-39).

As per claims 16-20, Haber et al teach a method of identifying data that

comprises a hash value generated from a one-way hash function and including the hash value and the time indication to the time stamp receipt (column 3, lines 10-65).

As per claim 21, Haber et al teach said time stamp request further includes an identification number associated with the requestor (column 3, lines 10-65 column 4, lines 8-39).

As per claim 22, Haber et al teach said message authentication code comprise a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenate together (column 3, lines 10-65).

As per claim 23, the examiner supplies the same rationale for the motivation as recited in the rejection of claim 15 to incorporate the teachings of Doyle within the system of Haber et al to include a second message authentication code. Haber et al teach said message authentication code comprise a digital sequence generated by application of a deterministic function to said time stamp receipt and said secret key concatenate together (column 3, lines 10-65). Therefore it would have been obvious that the second message authentication code also comprises a numeric representation.

As per claim 24, the examiner supplies the same rationale for the motivation as recited in the rejection of claim 15 to incorporate the teachings of Doyle within the system of Haber et al to include a second message authentication code. Haber et al

teach the step of validating said message authentication code includes recomputing said message authentication code at said outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code (see abstract). It is obvious that, because the second message authentication code comprises that concatenation of the first message authentication code and the secret keys, that the first message authentication code which was sent would be compared to the first authentication code which is a part of the second message authentication code.

As per claim 25, Haber et al teach the step of validating said message authentication code includes recomputing said message authentication code at said outside agency using said received time stamp receipt and said secret key and comparing the recomputed message authentication code to said received message authentication code (see abstract).

As per claim 26, Haber et al teach wherein the certifying step includes signing said message authentication code using a private signature key controlled by said outside agency (see abstract).

As per claim 27, Haber et al teach wherein the certifying step includes signing said time stamp receipt using a private signature key controlled by said outside agency (see abstract).

As per claim 28, Haber et al teach the step of transmitting said certified time stamp receipt to said requestor (column 4, line 8-26).

As per claim 49, Haber et al teach certifying said time stamp receipt at outside agency comprises signing said time stamp receipt with a private signature key (column 7, line 10).

As per claim 50, the examiner supplies the same rationale for the motivation as recited in the rejection of claim 41 to incorporate the teachings of Schneier within the system of Haber et al. Haber teaches that the key is a secret key and private signature keys are often referred to as secret keys in the art of cryptography.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael R Vaughan whose telephone number is 703-305-0354. The examiner can normally be reached on M-F 7:30-4:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MV
Michael R Vaughan
Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100